CLAIMS

What is claimed is:

1. A method for providing media content while preventing its unauthorized distribution, said method comprising:

transmitting from a client node to an administrative node a request for delivery of an instance of media content;

determining which content source of a plurality of content sources to provide delivery of said instance of media content, provided said client node is authorized to receive said instance of media content;

transmitting to said client node an access key and a location of said instance of media content of said content source;

transmitting from said client node to said content source a second request and said access key;

in response to receiving said second request and said access key, transferring said instance of media content from said content source to said client node;

transmitting from said client node to said administrative node an indicator indicating a successful transfer of said instance of media content from said content source to said client node; and

generating a transaction applicable to said client node and associated with said transfer of said instance of media content to said client node.

2. The method as recited in Claim 1, wherein said determining which content source of said plurality of content sources to provide delivery of said instance of media content further comprises:

determining which content source of said plurality of content sources is nearest to the physical location of said client node.

3. The method as recited in Claim 1, wherein said determining which content source of said plurality of content sources to provide delivery of said instance of media content further comprises:

determining which content source of said plurality of content sources contains said instance of media content.

4. The method as recited in Claim 1, wherein said access key is a time sensitive access key that becomes obsolete after a defined amount of time.

5. The method as recited in Claim 1, wherein said location of said instance of media content comprises an address.

6. The method as recited in Claim 5, further comprising:

changing said address after said transferring said instance of media content from said content source to said client node.

7. The method as described in Claim 1, wherein said instance of media content comprises a digital watermark or an embedded key.

8. The method as recited in Claim 1, wherein said instance of media content stored within a custom file system of memory coupled to said content source.

9. The method as recited in Claim 1, further comprising:

decrypting said instance of media content on said content source from an encryption local to said content source to an intermediate encryption via an intermediate encryption key received from said administrative node.

10. The method as recited in Claim 9, further comprising:

decrypting said instance of media content in said intermediate encryption at said client node via an intermediate decryption key received from said administrative node.

11. The method as recited in Claim 10, further comprising:

encrypting said instance of media content to an encryption local to said client node.

12. The method as recited in Claim 1, further comprising:

preventing a secure player application coupled to said client node from sharing said instance of media content with a second client node when said client node is unauthorized to do so.

13. The method as recited in Claim 1, further comprising:

disabling a secure player application coupled to said client node to prevent presentation of said instance of media content on said client node when said client node is unauthorized to do so.

14. The method as recited in Claim 1, further comprising:

enabling a secure player application coupled to said client node to present said instance of media content on said client node when said client node is authorized to do so.

15. The method as recited in Claim 1, further comprising:

authorizing said client node by verifying a secure player application and a client application are coupled to said client node.

16. The method as recited in Claim 14, wherein said client application coupled to said client node performs said decryption and said encryption related to said client node.

17. The method as recited in Claim 1, further comprising:

storing said instance of media content in a custom file system of memory coupled to said client node.

18. The method as recited in Claim 1, further comprising:

complying with a usage restriction applicable to said instance of media content on said client node via a usage compliance mechanism coupled to said client node.

19. A method for preventing unauthorized access to protected media disposed on a media storage device, said method comprising:

activating an autorun mechanism disposed on said media storage device in response to a device drive coupled with a client device receiving said media storage device, said autorun mechanism for initiating installing a compliance mechanism on said client device;

installing said compliance mechanism on said client device, said compliance mechanism communicatively coupled with said client device when installed thereon, said compliance mechanism for enforcing compliance with a usage restriction applicable to said protected media disposed on said media storage device;

obtaining control of a data input pathway operable on said client device;

preventing said protected media of said media storage device from being captured by an extractor mechanism via said data input pathway while enabling presentation of said protected media; and

initiating a communication session between said client device and a network from which said compliance mechanism is available, said network comprising a plurality of content sources.

20. The method as recited in Claim 19, further comprising:

updating said compliance mechanism on said client device from a content source of said plurality of content sources.

21. The method as recited in Claim 19, further comprising:

comparing said compliance mechanism present on said client device and said compliance mechanism available from said network; and

updating said compliance mechanism on said client device from a content source of said plurality of content sources.

22. The method as recited in Claim 19, further comprising:

invoking a presentation mechanism coupled with said client device, said presentation mechanism authorized in accordance with said compliance mechanism to present said protected media.

23. The method as recited in Claim 19, further comprising:

installing a presentation mechanism on said client device from a content source of said plurality of content sources to enable said client device to present said protected media, said presentation mechanism authorized in accordance with said compliance mechanism to present said protected media.

24. The method as recited in Claim 19, wherein said autorun mechanism is activated in response to detection of a usage restriction indicator disposed on said media storage device, subsequent to said device drive receiving said media storage device.

25. The method as recited in Claim 19, wherein said autorun mechanism is activated in response to detection of a selection of an icon representing said protected media.

26. The method as recited in Claim 19, wherein said usage restriction is a copyright restriction or a licensing agreement applicable to said protected media.

27. The method as recited in Claim 19, wherein said media storage device comprises a filter driver disposed thereon, said filter driver coupled to and operable in conjunction with said compliance mechanism for controlling said data input pathway.

28. The method as described in Claim 19, wherein said instance of media content comprises a digital watermark or an embedded key.

29. The method as recited in Claim 19, wherein said media storage device upon which said protected media is disposed is from a group consisting of:

a compact disk (CD), a mini CD, a digital versatile disk (DVD), a mini DVD, a compact flash card, a secure digital (SD) card, a memory stick, a digital audio tape (DAT), a digital video tape (DVT), a holographic storage object, a magneto-optical disk, a multi-layer fluorescent disk, an optical disk, and a magnetic disk.

30. A method for preventing unauthorized recording of media content, said method comprising:

transmitting from a client node to an administrative node a request for delivery of an instance of media content;

determining which content source of a plurality of content sources to provide delivery of said instance of media content, provided said client node is authorized to receive said instance of media content;

transmitting to said client node an access key and a location of said instance of media content of said content source;

transmitting from said client node to said content source a second request and said access key;

in response to receiving said second request and said access key, transferring said instance of media content from said content source to said client node;

activating a compliance mechanism in response to said client node receiving said instance of media content, said compliance mechanism coupled to said client node, said client node having a media content presentation application operable thereon and coupled to said compliance mechanism;

controlling a data path of a kernel-mode media device driver of said client node with said compliance mechanism upon detection of a kernel streaming mechanism operable on said client node; and

directing said media content from said kernel-mode media device driver to a media device driver coupled with said compliance mechanism, via said data path, for selectively restricting output of said media content.

31. The method as recited in Claim 30, wherein said determining which content source of said plurality of content sources to provide delivery of said instance of media content further comprises:

determining which content source of said plurality of content sources is nearest to the physical location of said client node.

32. The method as recited in Claim 30, wherein said determining which content source of said plurality of content sources to provide delivery of said instance of media content further comprises:

determining which content source of said plurality of content sources contains said instance of media content.

33. The method as recited in Claim 30, wherein said access key is a time sensitive access key that becomes obsolete after a defined amount of time.

34. The method as recited in Claim 30, wherein said location of said instance of media content comprises an address.

35. The method as recited in Claim 34, further comprising:

changing said address after said transferring said instance of media content from said content source to said client node.

36. The method as recited in Claim 30, further comprising:

preventing said instance of media content from being returned from said kernel-mode media device driver to a recording application coupled to said client node when recording said instance of media content violates a usage restriction applicable to said instance of media content.

37. The method as recited in Claim 30, further comprising:

allowing said media content to be returned from said kernel-mode device driver to a recording application coupled to said client system when recording said instance of media content complies with a usage restriction applicable to said instance of media content.

38. The method as recited in Claim 30, further comprising:

restricting said client node to have said media device driver implemented as a default media device driver.

39. The method as recited in Claim 30, further comprising:

accessing an indicator associated with said instance of media content for indicating to said compliance mechanism a usage restriction applicable to said media content.

40. The method as recited in Claim 30, wherein said kernel-mode media device driver is part of an operating system operable on said client system.

41. The method as recited in Claim 30 further comprising:

altering said compliance mechanism present on said client node from a content source of said plurality of content sources in response to a change in a usage restriction comprising a copyright restriction or licensing agreement applicable to said instance of media content.

42. A method of preventing unauthorized recording of media content, wherein said method comprising:

transmitting from a client system to an administrative system a request for delivery of an instance of media content;

determining which content source of a plurality of content sources to provide delivery of said instance of media content, provided said client system is authorized to receive said instance of media content;

transmitting to said client system an access key and a location of said instance of media content of said content source;

transmitting from said client system to said content source a second request and said access key;

in response to receiving said second request and said access key, transferring said instance of media content from said content source to said client system;

activating a compliance mechanism in response to receiving said instance of media content by said client system, said compliance mechanism coupled to said client system, said client system having a media content presentation application operable thereon and coupled to said compliance mechanism;

controlling a data output path of said client system with said compliance mechanism; and

directing said instance of media content to a custom media device coupled to said compliance mechanism via said data output path, for selectively restricting output of said media content.

43. The method as recited in Claim 42, wherein said determining which content source of said plurality of content sources to provide delivery of said instance of media content further comprises:

determining which content source of said plurality of content sources is nearest to the physical location of said client system.

44. The method as recited in Claim 42, wherein said determining which content source of said plurality of content sources to provide delivery of said instance of media content further comprises:

determining which content source of said plurality of content sources contains said instance of media content.

45. The method as recited in Claim 42, wherein said access key is a time sensitive access key that becomes obsolete after a defined amount of time.

46. The method as recited in Claim 42, wherein said location of said instance of media content comprises an address.

47. The method as recited in Claim 46, further comprising:

changing said address after said transferring said instance of media content from said content source to said client system.

48. The method as recited in Claim 42, wherein said instance of media content comprises a digital watermark or an embedded key.

49. The method as recited in Claim 42, further comprising:

preventing a recording application coupled to said client system from recording said instance of media content when said recording violates a usage restriction applicable to said instance of media content.

50. The method as recited in Claim 42, further comprising:

allowing a recording application coupled to said client system to record said instance of media content when said recording complies with a usage restriction applicable to said instance of media content.

51. The method as recited in Claim 42, further comprising:

restricting said client system to have said custom media device as a default media device.

52. The method as recited in Claim 42, further comprising:

accessing an indicator associated with said instance of media content indicating to said compliance mechanism a usage restriction applicable to said media content.

53. The method as recited in Claim 42, wherein said custom media device is an emulation of a custom media driver.

54. The method as recited in Claim 42, further comprising:

altering said compliance mechanism present on said client system from a content source of said plurality of content sources in response to a change in a usage restriction comprising a copyright restriction or licensing agreement applicable to said instance of media content.

55. A method of controlling interaction of deliverable media content, wherein said method comprising:

transmitting from a client system to an administrative node a request for delivery of an instance of media content;

determining which content source of a plurality of content sources to provide delivery of said instance of media content, provided said client system is authorized to receive said instance of media content;

transmitting to said client system an access key and a location of said instance of media content of said content source;

transmitting from said client system to said content source a second request and said access key;

in response to receiving said second request and said access key, transferring said instance of media content from said content source to said client system;

detecting a media player application coupled to a client system, said media player application for enabling said client system to present said instance of media content;

governing a function of said media player application that enables non-compliance with a usage restriction applicable to said instance of media content; and

controlling an output of said instance of media content by a compliance mechanism coupled to said computer system, said compliance mechanism enables compliance with said usage restriction applicable to said instance of media content.

56. The method as recited in Claim 55, wherein said determining which content source of said plurality of content sources to provide delivery of said instance of media content further comprises:

determining which content source of said plurality of content sources is nearest to the physical location of said client system.

57. The method as recited in Claim 55, wherein said determining which content source of said plurality of content sources to provide delivery of said instance of media content further comprises:

determining which content source of said plurality of content sources contains said instance of media content.

58. The method as recited in Claim 55, wherein said access key is a time sensitive access key that becomes obsolete after a defined amount of time.

59. The method as recited in Claim 55, wherein said location of said instance of media content comprises an address.

60. The method as recited in Claim 59, further comprising:

changing said address after said transferring said instance of media content from said content source to said client system.

61. The method as recited in Claim 55, wherein said instance of media content comprises a digital watermark or an embedded key.

62. The method as recited in Claim 55, wherein said controlling output of said instance of media content comprises diverting a data pathway of said media player application to a controlled data pathway controlled by said compliance mechanism.

63. The method as recited in Claim 55, further comprising:

attaching an indicator to said media file prior to delivery to said computer system, said indicator for indicating to said compliance mechanism that said instance of media content originated from said content server.

64. The method as recited in Claim 63, further comprising:

encrypting said instance of media content and said indicator prior to delivery of said instance of media content to said client system.

65. The method as recited in Claim 55, further comprising:

permitting said media player application to present said instance of media content, provided said media player application complies with said usage restriction.

66. The method as recited in Claim 55, further comprising:

installing said compliance mechanism onto said client system from a content server of said plurality of content servers.

67. The method as recited in Claim 55, further comprising:

altering said compliance mechanism using a content server of said plurality of content servers in response to changes in said usage restriction.

68. The method as recited in Claim 55, further comprising:

installing a custom media player application on said client system and configured to be operable when said media player application does not comply with said usage restriction.

69. The method as recited in Claim 55, further comprising:

verifying the presence and the integrity of authorization data stored on said client system by said compliance mechanism prior to delivery of said instance of media content to said client system.

70. The method as recited in Claim 55, further comprising:

monitoring said instance of media content during its presentation by said compliance mechanism for compliance with said usage restriction.

71. The method as recited in Claim 55, wherein said instance of media content is delivered to said client system via a hypertext transfer protocol file delivery.

72. The method as recited in Claim 55, wherein said usage restriction is a copyright restriction or a licensing agreement applicable to said instance of media content.

73. A method for controlling presentation of media content on a media storage device, said method comprising:

verifying presence of a content presentation mechanism and a usage compliance mechanism on a client system, said usage compliance mechanism including a file system filter driver for controlling data reads associated with said media content;

permitting presentation of said media content via said client system provided said usage compliance mechanism is present on said client system, said client system is communicatively coupled with a network, and a source node of said network authorizes presentation of said media content, said network comprises a plurality of source nodes; and

presenting said media content via said content presentation mechanism that is communicatively coupled with said usage compliance mechanism, said content presentation mechanism enabled to present said content when communicatively coupled with said source node.

74. The method as recited in Claim 73, further comprising:

installing said usage compliance mechanism on said client system when said usage compliance mechanism is not present on said client system; and

installing said content presentation mechanism on said client system when said content presentation mechanism is not present on said client system.

75. The method as recited in Claim 74, wherein said media storage device comprises an autorun mechanism disposed thereon that initiates installation of said usage compliance mechanism and said content presentation mechanism on said client system in response to said client system receiving said media storage device and said usage compliance mechanism and said content presentation mechanism are not present on said client system.

76. The method as recited in Claim 73, further comprising:

encrypting said media content prior to disposal of said content on said media storage device.

77. The method as recited in Claim 76, wherein said encrypting comprises a first encryption applied to said media content and a second encryption applied to said first encryption and associated content.

78. The method as recited in Claim 76, wherein said encrypting comprises a unique first encryption applied to each instance of media content when a plurality of media content is disposed on said media storage device and a unique second encryption is applied to each said unique first encryption and associated content.

79. The method as recited in Claim 78, further comprising:

decrypting said second encryption with said file system filter driver using a second decryption key stored on a source node of said plurality of source nodes.

80. The method as recited in Claim 78, further comprising:

decrypting said first encryption with said media content presentation mechanism using a first decryption key stored on a source node of said plurality of source nodes concurrent with said presenting.

81. The method as recited in Claim 73, further comprising:

affixing a unique identifier on said media storage device.

82. The method as recited in Claim 81, wherein said unique identifier is a serial number generated prior to or during disposition of said media content on said media storage device.

83. The method as recited in Claim 82, further comprising:

watermarking said content via said content presentation mechanism during decryption of a first encryption applied to said media content, said content presentation mechanism further causing said unique identifier to be watermarked onto an outgoing data stream containing said media content.

84. The method as recited in Claim 73, further comprising:

updating said content presentation mechanism via a source node of said plurality of source nodes.

85. The method as recited in Claim 73, further comprising:

updating said usage compliance mechanism via a source node of said plurality of source nodes.

86. The method as recited in Claim 73, further comprising:

determining which source node of said plurality of source nodes to update said content presentation mechanism or said usage compliance mechanism.

87. The method as recited in Claim 86, wherein said determining further comprises:

determining which source node of said plurality of source nodes is nearest to the physical location of said client system.

88. The method as recited in Claim 86, wherein said determining further comprises:

determining which source node of said plurality of source nodes contains said content presentation mechanism or said usage compliance mechanism.